I Claim:

1. A secure file transfer system hosted on a server computer connected to a computer network and accessible by users via client computers connected to the computer network and running a hypertext viewer, the system including:

a request page including a request submission object operable by a user visiting the request page;

a destination specification page including a destination specification tool with which the user specifies a destination of the secure file transfer, the destination specification page further including a transfer initiation object operable by the user to initiate transmission of the document;

a client side application sent to the client computer upon operation by the user of the transfer initiation object, the client side application including:

a file picker prompting the user to select a file for transfer to the destination, the client side application first sending the file to the server computer in blocks determined by a size of the file;

a key generator that generates a shared secret key and shares the key with the system on the server computer; and

an encrypter, including essential parameters for encryption, that encrypts the file in its entirety and also encrypts each block of the file as the client side application sends the file in blocks to the server computer; and

a notifier that notifies a recipient user at the destination that the file awaits pickup on the server computer.

2. The system of claim 1 wherein the hypertext viewer is a web browser.

3. The system of claim 1 wherein the client-side application is a java applet.

4. The system of claim 1 wherein the first encryption method is an elliptical encryption method.

5. The system of claim 2 wherein the parameters for the elliptical encryption method include q, a, b, r, and G.

6. The system of claim 1 wherein the second encryption method is a public key agreement scheme.

7. The system of claim 4 wherein the second encryption method is the Mendez-Qu-Vanstone public key agreement scheme with cofactor multiplication.

8. The system of claim 1 further including a secure document manager that displays statistics relating to a user's usage of the system.

9. The system of claim 6 wherein the manager displays a list of secure documents awaiting pickup.

10. The system of claim 1 wherein the notifier sends an e-mail message to the recipient.

11. The system of claim 8 wherein the e-mail message includes a hypertext link to the secure document awaiting pickup.

12. A secure file transfer system hosted on a server computer connected to a computer network and accessible by users via client computers connected to the computer network and running a desktop software application, the system including:

a request page including a request submission object operable by a user visiting the request page;

a destination specification page including a destination specification tool with which the user specifies a destination of the secure file transfer, the destination specification page further including a transfer initiation object operable by the user to initiate transmission of the document;

a desktop software application sent to the client computer upon operation by the user of the transfer initiation object, the desktop software application including:

a file picker prompting the user to select a file for transfer to the destination, the desktop software application first sending the file to the server computer in blocks determined by a size of the file;

a key generator that generates a shared secret key and shares the key with the system on the server computer; and

an encrypter, including essential parameters for encryption, that encrypts the file in its entirety and also encrypts each block of the file as the desktop software application sends the file in blocks to the server computer; and

a notifier that notifies a recipient user at the destination that the file awaits pickup on the server computer.

13. The system of claim 12 wherein the desktop software application is a Windows based software application.

14. The system of claim 12 wherein the first encryption method is an elliptical encryption method.

15. The system of claim 14 wherein the parameters for the elliptical encryption method include q, a, b, r, and G.

16. The system of claim 12 wherein the second encryption method is a public key agreement scheme.

17. The system of claim 16 wherein the second encryption method is the Mendez-Qu-Vanstone public key agreement scheme with cofactor multiplication.

18. The system of claim 12 further including a secure document manager that displays statistics relating to a user's usage of the system.

19. The system of claim 18 wherein the manager displays a list of secure documents awaiting pickup.

20. The system of claim 12 wherein the notifier sends an e-mail message to the recipient.

21. The system of claim 20 wherein the e-mail message includes a hypertext link to the secure document awaiting pickup.

22. A secure file transfer method executed as a software application on a server computer connected to a computer network and accessible by users via client computers connected to the computer network and running a web browser, the method including the steps of:

receiving a request from a user for secure file transfer;

sending an Java applet to the client computer with parameters for first and second methods of encryption, the first method of encryption not requiring additional information from either side of the transfer and a shared secret key for the second method of encryption being sent in encrypted form;

receiving and decrypting with the Java applet the shared secret key for the second of encryption;

encrypting a file to be transferred with the Java applet by applying the first method of encryption;

breaking the file into blocks with the Java applet;

encrypting each block with the Java applet by applying the second method of encryption and sending the block to the server with the Java applet;

decrypting the encrypted file blocks and assembling into a decrypted file with the shared secret key as they arrive at a recipient computer;

storing the encrypted file on a mass storage device; and

notifying a recipient at a destination of the file that the file awaits pickup on the server computer.

23. The method of claim 22 wherein the step of applying the first method of encryption includes the substep of applying an elliptical encryption method.

24. The method of claim 22 wherein the step of applying the second method of encryption includes applying the Mendez-Qu-Vanstone public key agreement scheme with cofactor multiplication.

25. The method of claim 22 wherein the step of notifying includes sending an e-mail message to the recipient.

26. The method of claim 25 wherein the e-mail message includes a hypertext link to the file.

27. The method of claim 22 further including the step of displaying user usage statistics.

28. The method of claim 22 further including the step of providing a transfer request page from which the user requests the file transfer.

29. The method of claim 28 wherein the step of providing a transfer request page includes providing a document forwarding request.

30. A secure file transfer system hosted on a main server computer connected to a computer network and accessible by users via client computers connected to the computer network, the system including a file picker with which a sending user specifies a file to be transferred to a recipient, a file encrypter in communication with the file picker that encrypts the specified file to produce an encrypted file, a file sender that transfers the encrypted file to an encrypted file storage location, and a notifier that alerts a recipient of the file that the encrypted file awaits pickup.

31. The system of claim 30 wherein the file resides on a mass storage device on a storage server computer connected to the computer network.

32. The system of claim 31 wherein the storage server is closely associated with the main server and provides online remote storage for the sending user.

33. The system of claim 31 wherein the file picker presents the sending user with a list of files present on the storage server and accessible to the sending user.

34. The system of claim 30 wherein the storage server is closely associated with the sending user's computer and the file picker is part of a Java applet sent to the sending user's computer by the system, the file picker including a user interface tying into the sending user computer's operating system so that the user can browse storage devices closely associated with the sending user's computer.

35. The system of claim 34 wherein the storage server is a storage device that is physically part of the sending user's computer.

36. The system of claim 34 wherein the storage server is a volume directly accessible by the sending user's computer but inaccessible to the main server without the sending user's use of the file picker.

37. The system of claim 30 wherein the encrypter is a client-side routine that is part of a Java applet sent to the sending user's computer by the system, the encrypter including essential parameters for encryption.

38. The system of claim 37 wherein the encrypter uses elliptical encryption.

39. The system of claim 30 wherein the file sender breaks the encrypted file into blocks and sends the blocks to the storage location.

40. The system of claim 39 wherein the file sender interacts with the file encrypter so that the file encrypter encrypts each block of the encrypted file as the file sender sends the block to the storage location.

41. The system of claim 40 further including a block decrypter between the file sender and the storage location that decrypts each block of the encrypted file as it receives the blocks from file sender.

42. The system of claim 39 further including an assembler between the file sender and the storage location that reassembles the blocks into the encrypted file.